El Uso de Técnicas de Ingeniería Social Integradas a Inteligencia Artificial para Atacar Objetivos

Ana Sofía Zalazar

ISI (UTN-FRT), Rivadavia 1050, San Miguel de Tucumán, 4000, Argentina
anazalazar@doc.frt.utn.edu.ar

Resumen. En este trabajo se aborda la creciente amenaza en ciberseguridad derivada del empleo de Inteligencia Artificial (IA) en el uso de técnicas de Ingeniería Social (IS). La convergencia entre ambas disciplinas ha creado un escenario donde la sofisticación de los algoritmos de IA se aprovecha para manipular a usuarios y realizar ciberataques personalizados. En respuesta a esta problemática, se proponen soluciones proactivas, destacando la implementación de medidas de seguridad avanzadas, la concientización continua de los usuarios y la adaptación de estrategias de ciberseguridad al contexto de una organización. Una parte sustancial de este trabajo se dedica a definir IS e IA, y la aplicabilidad de diferentes técnicas en el campo de la ciberseguridad. Se destaca la utilización de algoritmos avanzados, como los algoritmos de inteligencia artificial generativa, que permiten la personalización de técnicas, adaptándose a las características y preferencias individuales de las personas, lo que incrementa la probabilidad de éxito de los ciberataques. Finalmente, el trabajo presenta propuestas concretas relacionadas con los conceptos tratados y la ciberseguridad.

Palabras Clave: Inteligencia Artificial, Ingeniería Social, Ciberseguridad, Ciberataques.

1 Introducción

El mayor deseo de los ciberdelincuentes cuando lanzan un ataque dirigido es que este consiga su objetivo, es decir, propagar código malicioso o hacer que las víctimas compartan información sensible o de acceso restringido. Un ciberataque es cualquier acción que atente contra la confidencialidad, integridad o disponibilidad de un sistema informático, red o dispositivo [8].

Se llama Ingeniería Social (IS) a las diferentes técnicas de manipulación que usan los ciberdelincuentes para acceder a los recursos informáticos a través de los usuarios, que se consideran el eslabón más débil de la cadena de seguridad de la información [5]. Las tácticas de IS inducen a individuos, también llamadas víctimas, a divulgar información confidencial, instalar aplicaciones no autorizadas, acceder a sitios web potencialmente peligrosos, transferir fondos a entidades delictivas u incurrir en otros actos que comprometan su seguridad personal o de la organización a la que pertenecen. La IS utiliza la manipulación psicológica y aprovecha los errores o debilidades humanas en lugar de las vulnerabilidades técnicas o digitales de los sistemas, a veces se denomina *"hacking humano"* [5, 6].

Para los ciberdelincuentes, el uso de la tecnología de Inteligencia Artificial (IA) para lanzar ciberataques se está volviendo muy popular, puesto que esta asegura una mayor eficacia y efectividad del ciberataque. El uso de la IA para lanzar ciberataques se refiere a la utilización de algoritmos y sistemas informáticos para realizar tareas que normalmente requieren del capital humano para llevarse a cabo, como por ejemplo confeccionar un correo electrónico o alterar una fotografía. No obstante, gracias al aprendizaje automático integrado dentro de la IA, esta tecnología es capaz de analizar gran cantidad de datos proveniente de diferentes fuentes, como motores de búsquedas y redes sociales, para detectar vulnerabilidades y brechas de seguridad en los sistemas informáticos y usuarios de una organización. De manera más eficiente y a gran escala, y combinando técnicas de IS se puede dirigir ataques específicos hacia un determinado objetivo (persona u organización). Asimismo, la IA puede ayudar a contrarrestar los ataques provocados por ciberdelincuentes.

Este trabajo, resultado del análisis de la situación actual, se encuentra organizado de la siguiente manera. A continuación, se definen “Ingeniería Social” e “Inteligencia Artificial”. En la “Situación Actual”, se presenta un análisis de los ataques cibernéticos que se han dado a conocer públicamente en Argentina entre julio de 2020 y julio de 2023. En la sección de “Consideraciones”, se evalúa algunos desafíos del uso de Inteligencia Artificial en el campo de la ciberseguridad. Finalmente se presentan las “Propuestas” que son recomendaciones para prevenir ciberataques, y las “Conclusiones” de este trabajo.

2 Ingeniería Social

La Ingeniería Social (IS) es el término que se utiliza para la práctica ilegítima de obtener acceso a información confidencial o sistemas seguros a través de la manipulación de usuarios legítimos [12]. Las técnicas de manipulación de IS son utilizadas para lograr que ciertas personas o víctimas de ataques realicen alguna acción que permita a los atacantes realizar su cometido. Las técnicas más comunes son [5]:

- *El cebo*: Atraer a la víctima con algo que le resulte atractivo, como un premio, una oferta falsa o revelar información confidencial.
- *El pretexto*: Inventar una situación que requiera la ayuda de la víctima, haciéndola sentir obligada a colaborar.
- *La autoridad*: Fingir ser una figura de autoridad para que la víctima siga las instrucciones sin cuestionarlas.
- *La escasez*: Crear una sensación de urgencia para que la víctima actúe rápidamente sin pensar con claridad.
- *La validación social*: Utilizar la aprobación de otros para influir en la decisión de la víctima.

Otros mecanismos de manipulación que se están dando con mayor frecuencia en los últimos años son: “*phishing”* que son correos electrónicos ilegítimos que tiene el propósito de obtener información de la víctima o que se descargue un software malicioso; “*vishing”* que busca obtener información sensible a través de una llamada telefónica; “*baiting”* que consiste en depositar dispositivos maliciosos públicos, como

pendrives, memorias y cargadores, que tiene código malicioso que se ejecutan al ser accedidos; "*spear-phishing"* que son correos dirigidos a alguien que tiene, por ejemplo, un determinado cargo o maneja información sensible en una empresa; "*hunting"* es un tipo de ataques buscan afectar al mayor número de usuarios realizando, únicamente, una comunicación masiva; "*farming"* es una técnica que realizan varias comunicaciones con las víctimas hasta conseguir la mayor cantidad de información posible; "*robo de cuentas"* orientado a correos electrónicos o redes sociales con la finalidad de cometer hechos ilícitos y comprometer a los contactos de las víctimas, como pedir dinero, enviar software malicioso u obtener información personal; y "*pretexting"* es una de las técnicas más elaboradas porque el atacante debe generar un buen escenario para poder robar información importante y sensible, para estos busca ganarse la confianza de la víctima generando un vínculo. [1, 11].

A pesar de ser múltiples y varias las técnicas utilizadas por los ciberdelincuentes para manipular a sus víctimas suelen aprovecharse de serie de principios básicos, por ejemplo, el principio al respecto a la autoridad, la voluntad de ayudar a otros, el deseo de mantener un producto o servicio, el temor a perder el respeto social cuando se realizan chantajes informática, la gratuidad de un producto o servicio promocionado y la curiosidad ante novedades y noticias [7]. Generalmente, los ciberdelincuentes más sofisticados investigan a un usuario o una organización, generan un perfil y dirigen un ataque de IS basado en estos principios básicos.

En otras palabras, la IS se ha convertido en una herramienta fundamental para los ciberdelincuentes, quienes la utilizan para explotar las vulnerabilidades psicológicas y sociales de las personas [11]. Los ciberatacantes que realizan estos tipos de técnicas conocen estas vulnerabilidades personales y saben que las víctimas son propensas a cometer errores humanos como hacer clic en enlaces de correos maliciosos, usar contraseñas débiles o descuidar un dispositivo con datos confidenciales o firmas digitales. Además, en presencia de técnicas muy sofisticadas las personas pueden ser engañadas para revelar información confidencial o para brindar una puerta de acceso a un archivo malicioso o conexión indeseada. Las personas generalmente no consideran que podrían ser un objetivo de un ciberatacante, además, tienen una confianza excesiva en los demás y generalmente se encuentran desactualizadas sobre las últimas tácticas y técnicas de ciberseguridad, mientras que las amenazas a la ciberseguridad se encuentran en continua evolución.

3 Inteligencia Artificial

La Inteligencia Artificial (IA) es una poderosa herramienta que puede utilizarse para integrarse a las técnicas de Ingeniería Social (IS), por su inmensa capacidad de automatización y análisis de gran volumen de datos. La IA puede analizar grandes cantidades de datos de un objetivo (persona u organización) y generar nuevo contenido, con eficiencia, precisión y rapidez, que puede ser utilizado por los atacantes para orientar un ciberataque.

La IA como disciplina tiene el propósito de crear máquinas que imiten la inteligencia humana para realizar tareas, y que pueden mejorar conforme recopilen información [15]. Por ejemplo, el aprendizaje automático ("*machine learning"*) es una rama de IA, que permite la recolección automática de información y tomar decisiones

aplicando algoritmos a los datos recolectados. El aprendizaje automático tiene fuertes vínculos con técnicas matemáticas que permiten un proceso de extracción de información, descubrimiento de patrones y deducción de conclusiones a partir de datos de entrada, y esto es muy útil para dirigir ciberataques.

La IA se puede utilizar para mejorar la eficacia de las técnicas de IS al automatizar tareas como la recopilación de información y la creación de mensajes o contenido personalizado [17]. En otras palabras, la IA se puede utilizar para recopilar información de diversas fuentes sobre las víctimas, como base de datos públicas y las redes sociales, con el objetivo de detectar sus intereses y aprender sobre su contexto. Esta información se puede utilizar para crear mensajes que sean más convincentes para las víctimas o para mejorar la técnica del ciberataque. Inclusive, existen programas que utilizan algoritmos de IA que permiten automatizar la generación con alta fidelidad de contenido multimedia y páginas web, utilizando información dispuesta de manera pública en Internet [14].

Se llaman "*deepfake*" (ultra falsos) a los archivos de videos, imágenes o audio manipulados por IA para que parezcan reales. Para los "*deepfake"* se utiliza aprendizaje profundo, una rama avanzada de IA, que mediante múltiples capas de algoritmos de aprendizaje automático generar contenido sintético que imita la apariencia y la voz de una persona, lo que resulta muy convincente, y es un nuevo desafío para ciberseguridad [3]. En los últimos años, hubo un aumento de perfiles falsos o personas sintéticas en redes sociales, como resultados de algoritmos que imitan comportamientos humanos en estas plataformas, estableciendo conexiones y recopilando información de otros usuarios.

Con la proliferación de algoritmos de código abierto y el aumento de la potencia computacional, la implementación de IA se volvió más accesible y especializada. El crecimiento de la adopción de estos algoritmos y el potencial impacto en la sociedad han generado un debate importante en los últimos años, impulsando la investigación de métodos para combatir su uso indebido.

Por otro lado, la aparición de ataques dirigidos por reconocimiento facial se volvió otro desafío, ya que utiliza algoritmos biométricos para identificar objetivos, adaptando tácticas según la información recopilada. Estas técnicas resaltan la capacidad de estos sistemas para adaptarse y manipular a los usuarios de manera más eficiente [3, 7].

El phishing inteligente utiliza la capacidad de la IA para analizar patrones de comportamiento, personalizando mensajes de suplantación de identidad y aumentando su persuasión. La inteligencia artificial generativa se puede utilizar para crear correos electrónicos de phishing que se dirijan a personas específicas. Por ejemplo, se puede utilizar para crear correos electrónicos que parecen provenir del jefe de la víctima o de un compañero de trabajo [1].

4 Situación Actual

Las amenazas a la seguridad de la información evolucionan, y cada vez más los ataques se revisten de inteligencia.

Johnson y otros señalan que los ataques cibernéticos han aumentado en frecuencia y sofisticación, presentando desafíos significativos para las organizaciones que deben defender sus datos y sistemas de los actores capaces de realizar amenazas. Estos actores

van desde atacantes individuales y autónomos hasta grupos con buenos recursos que operan de manera coordinada como parte de una empresa criminal o en nombre de un estado-nación. Los actores de amenazas pueden ser persistentes, motivados y ágiles, y utilizan una variedad de tácticas, técnicas y procedimientos para comprometer sistemas, interrumpir servicios, cometer fraude financiero y exponer o robar propiedad intelectual y otra información confidencial [10].

Durante el periodo comprendido entre julio de 2020 y julio de 2023, se reportaron públicamente 49 ataques cibernéticos en organizaciones públicas y privadas de Argentina [13]. El 49% de estos incidentes de seguridad se clasificaron como *"ransomware"*, que consiste en el bloqueo al acceso a los datos o sistemas y en el pedido de un pago para la liberación de estos recursos informáticos, y este ataque generalmente inicia con correo electrónico del tipo "*phishing*". El 24% de los casos publicados se clasificaron como "*denial of service*" (DoS), que es un tipo de ataque cibernético diseñado para interrumpir o denegar el acceso legítimo a un servicio, recurso o sistema informático. El 22% de los ataques reportados corresponden al tipo "*databreach*" (violación de datos), el cual consiste en el acceso y la filtración de información confidencial, sensible o privada de manera no autorizada, y estos ataques generalmente violan la Ley 25.326 de Argentina sobre Protección de Datos Personales. El resto de los incidentes publicados corresponden a la presencia de intrusos y accesos no autorizados a los sistemas.

Generalmente, los expertos en seguridad tienen dificultades para rastrear e identificar la puerta de entrada de un ciberatacante y los factores de un ciberataque. Sin embargo, las organizaciones no deben olvidarse de que el eslabón más débil de su infraestructura son los usuarios, y que pueden ser la puerta de entrada de numerosos ataques masivos a la ciberseguridad. Es precisamente que la IS se centra en este eslabón para realizar un ciberataque.

En Argentina se registraron nueve millones de bloqueos de intentos de *"phishing"* durante el 2022 y una cifra que a mediados del 2023 se multiplicó por ocho en relación con el período anterior [3].

La combinación de Ingeniería Social (IS) e Inteligencia Artificial (IA) se puede producir en la preparación de un engaño dirigido a un usuario, y puede ser altamente eficaz. Cuanto más realista parezca el mensaje y más confiable sea la fuente, más propenso será el usuario para creer en él. En consecuencia, si el atacante logra que el engaño sea convincente y bien dirigido, aumentan las posibilidades de que tenga éxito en sus objetivos, ya sea la reproducción de un programa malicioso o la exposición de información confidencial [4].

La IA es una herramienta o arma poderosa que se puede utilizar para preparar los ciberataques. Es importante ser consciente de cómo se puede utilizar la IA y la IS, para tomar medidas que protejan a las personas y organizaciones en materia de ciberseguridad.

5 Consideraciones

Los algoritmos de Inteligencia Artificial (IA) pueden ser utilizados tanto por los ciberdelincuentes para dirigir sus ataques, como por las personas y organizaciones para

proteger sus sistemas. La IA puede ayudar al ampliar la supervisión y detección de comportamientos sospechosos en una organización y que el personal de seguridad pueda reaccionar ante nuevas situaciones. Por otro lado, los sistemas que implementan IA pueden aprender con el tiempo a responder mejor a las amenazas, ya que pueden detectar desviaciones de comportamiento normal de un sistema o recurso informático [17].

El aprendizaje automático y el aprendizaje profundo son altamente eficaces en diversas áreas de la ciberseguridad, abordando problemas como el filtrado de spam, la detección de *"botnets"* (red de robot informáticos), anomalías de red y comportamientos anormales de los usuarios. El aprendizaje profundo ha demostrado mejoras notables en la detección de código y de intrusiones en comparación con las soluciones existentes [18].

En el ámbito de la prevención del "*phishing"*, se pueden implementar sistemas de detección de intrusiones y evaluar hipervínculos a sitios no deseados, pero presentan limitaciones, como la incapacidad para evitar que los usuarios accedan a enlaces maliciosos o proporcionen datos confidenciales.

Por otro lado, los algoritmos de IA pueden ser soluciones apropiadas para abordar técnicas de IS en el uso del correo electrónico. Existen algoritmos que clasifican automáticamente los correos electrónicos recibidos como *"spam"*, además, pueden detectar actividad inusual en cuentas comprometidas, prevenir la suplantación de dominio y alertar sobre sitios web suplantados o direccionamiento a páginas no deseadas [1].

Sin embargo, la aplicación de IA también enfrenta algunos desafíos de seguridad. Por ejemplo, los ciberataques dirigidos a algoritmos de IA son una preocupación en el área, debido a la existencia de sistemas que manipulan las entradas para engañar a los modelos de aprendizaje automático. El "*envenenamiento de datos*" es el resultado de contaminar la información de entrenamiento de modelos de IA para inducir comportamientos incorrectos. El "*robo de modelos*" es otra técnica que busca duplicar algoritmos o recuperar datos de entrenamiento, mediante el examen de la caja negra. Como consecuencia, los algoritmos de IA pueden realizar una clasificación incorrecta de la información lo que podría provocar falsos positivos o falsos negativos lo que representa también un problema significativo, sobrecargando al personal de seguridad informática o evitando la detección de amenazas [18]. A pesar de estos desafíos, cada vez más organizaciones utilizan las técnicas de IA para la ciberseguridad.

6 Propuestas

Los ciberdelincuentes se aprovechan de las vulnerabilidades más comunes en sistemas informáticos, que incluyen problemas de configuración en puertos de comunicación, incompatibilidad y desactualización tecnológica, falta de autenticación y autorización adecuadas, y carencia de cifrado en la transmisión de datos. Para evitar estos tipos de incidentes de seguridad es fundamental que las organizaciones implementen buenas prácticas de seguridad, como las recomendaciones y controles de ISO/IEC 27000:2022 [9].

Adicionalmente, medidas como la autenticación múltiple, el cifrado de datos y las auditorías periódicas son recomendables para mitigar los riesgos de incidentes de

seguridad en los sistemas informáticos. Además, se recomienda implementar algoritmos de validación y saneamiento para garantizar la seguridad de los datos que se comparten entre diferentes sistemas interoperables [16]. El saneamiento es una técnica utilizada para limpiar datos sensibles de una organización o datos potencialmente maliciosos y no deseados de una fuente antes de ser utilizados y almacenados en un sistema.

Aunque estas propuestas para fortalecer la infraestructura tecnológica son solo algunas pautas generales, es importante considerar las necesidades y características específicas de cada organización. Las organizaciones deberán contar con mecanismos de monitoreo y control de todos los puertos de conexión (servidores, dispositivos de red, etc.) para detectar el tráfico inadecuado de datos y para garantizar sistemas informáticos robustos y resistentes a ataques cibernéticos. Además, la realización de planes de contingencias y el mantenimiento de copias de seguridad regulares son prácticas cruciales que pueden automatizarse en una organización [9].

Por otro lado, se propone implementar un programa de concientización y capacitación para todos los niveles de una organización, sobre la privacidad en redes sociales, tanto profesionales como personales, y las diferentes técnicas de IS. Los usuarios deberían aprender a implementar políticas de contraseñas robustas y únicas, y siempre que sea posible utilizar la autenticación en dos pasos, que añade una capa de seguridad adicional mediante códigos temporales, lo que dificulta el acceso indebido incluso si se compromete las claves.

Tanto las organizaciones como las personas que conforman las mismas, deben conocer la importancia de mantener actualizados los dispositivos y los recursos informáticos con las últimas versiones y parches de seguridad. Las personas se olvidan de que muchas veces la información laboral y los archivos de una organización terminan siendo compartidos en una nube pública, mensajería instantánea, o servicios de correos gratuitos, por lo que se recomienda reforzar la conciencia de utilizar los canales institucionales y evitar compartir información confidencial utilizando estos tipos de herramientas.

Los usuarios deben ser escépticos de la información que se comparte en Internet, es decir, verificar la autenticidad de destinatarios, canales y herramientas de comunicación, y sobre todo no compartir información sensible en canales no formales.

Finalmente, se recomienda cultivar hábitos de seguridad en línea para toda la organización, con mensajes informativos para cerrar sesión después de usar dispositivos y ser cauteloso con las fuentes de información, con el objetivo de fortalecer la defensa contra posibles amenazas cibernéticas [2].

7 Conclusiones

En este trabajo se aborda el empleo de técnicas de Ingeniería Social (IS) e Inteligencia Artificial (IA) con fines ofensivos, que representan una creciente amenaza en el ámbito de la ciberseguridad. La convergencia de la IS y la IA ha generado un panorama donde la IA se utiliza de manera sofisticada para manipular y engañar a usuarios con el objetivo de acceder a información sensible o comprometer sistemas.

La IA, con su gran capacidad para aprender patrones de comportamiento y adaptarse a nuevas situaciones, ha potenciado las técnicas de IS. A través de algoritmos

avanzados, la IA puede analizar grandes cantidades de datos para personalizar ataques, creando mensajes o interacciones que se ajustan específicamente a las características y preferencias de sus objetivos (personas y organizaciones). Este nivel de personalización aumenta significativamente la efectividad de los ciberataques, ya que las víctimas son más propensas a caer en engaños cuando la información parece legítima y se adapta a sus perfiles.

En este contexto, la defensa contra estas amenazas requiere enfoques proactivos que incluyan la implementación de medidas avanzadas de seguridad, la concientización constante de los usuarios y la adaptación de estrategias de ciberseguridad para hacer frente a la evolución continua de estas tácticas. La colaboración entre expertos en ciberseguridad, desarrolladores de IA y profesionales de la psicología en el campo de IS se vuelve esencial para anticipar y contrarrestar las complejas interacciones entre estas disciplinas, protegiendo así la integridad de la información y fortaleciendo la seguridad en línea.

Finalmente, en este trabajo se abordan medidas básicas de seguridad para todos los niveles de una organización, y se presentan sugerencias y recomendaciones para prevenir amenazas cibernéticas.

References

1. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.
2. Argentina (2023). ¿Qué es la ingeniería social y cómo me protejo? Recuperado de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte.
3. Avolio, M. (2023). La inteligencia artificial aceleró una “epidemia de phishing” en la región. Télam. Recuperado de https://www.telam.com.ar/notas/202309/638582-inteligencia-artificial-epidemia-phishing-argentina.html.
4. Borghello, C. (2009). El arma infalible: la Ingeniería Social. Eset Latinoamérica.
5. Hadnagy, C. (2011). Ingeniería social: el arte del hacking personal. Ediciones Anaya Multimedia.
6. IBM (2023). ¿Qué es la ingeniería social? Recuperado de https://www.ibm.com/es-es/topics/social-engineering.
7. Instituto Nacional de Ciberseguridad (INCIBE). (2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. Recuperado de https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse.
8. Instituto Nacional de Ciberseguridad (INCIBE). (2020). Guía de ciberataques. Todo lo que debes saber a nivel usuario. Madrid: Oficina de Seguridad Interna y Ciberseguridad. Recuperado de: https://www.incibe.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf.
9. Organización Internacional de Normalización [ISO] e International Electrotechnical Commission [IEC]. (2022). Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27000:2022).
10. Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). Guide to cyber threat information sharing. NIST Special Publication, 800(150).

11. López Grande, C. E. (2015). Ingeniería social: el ataque silencioso. Revista Tecnológica: no. 8. Recuperado de http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf.
12. Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. John Wiley & Sons.
13. Parello, M. (2023). Ciberincidentes relevantes en Argentina. Recuperado de https://time.graphics/es/line/630567.
14. Ríos, J. (2023). Cómo evitar ser víctima de ciberataques hechos con inteligencia artificial. Infobae. Recuperado de https://www.infobae.com/tecno/2023/08/05/como-evitar-ser-victima-de-ciberataques-hechos-con-inteligencia-artificial/.
15. Russell, S. J., & Norvig, P. (2016). Artificial intelligence: a modern approach. Pearson.
16. Sánchez, C. (2019). Interoperabilidad en la Gestión Pública.
17. Sardanyés, E. (2023). Ejemplos de ciberataques lanzados con Inteligencia Artificial. Esedsl. Recuperado de https://www.esedsl.com/blog/ejemplos-de-ciberataques-lanzados-con-inteligencia-artificial .
18. Truong, T. C., Zelinka, I., Plucar, J., Čandík, M., & Šulc, V. (2020). Artificial intelligence and cybersecurity: Past, presence, and future. In Artificial intelligence and evolutionary computations in engineering systems (pp. 351-363). Springer Singapore.